PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	)
	)
Hursey et al.	) Art Unit: 2131
	)
Application No. 09/912,391	) Examiner: Henning, Matthew T.
	)
Filed: 07/26/2001	) Atty. Docket No.
	) NAI1P462/01.059.01
For: DETECTING E-MAIL PROPAGATED MALWARE	)
	) Date: 12/05/2007
	)
	)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

REPLY BRIEF (37 C.F.R. § 41.37)

This Reply Brief is being filed within two (2) months of the mailing of the Examiner's Answer mailed on 10/05/2007.

Following is an issue-by-issue reply to the Examiner's Answer.

Issue # 1:

The Examiner has objected to the specification as failing to provide proper antecedent basis for the claimed subject matter.

The Examiner has argued that "[t]he claim limitations regarding identifying whether (i), (ii), and (iii) in combination is not supported by the specification." Appellant respectfully disagrees and points out that page 6, lines 12-13 of the specification states that "the anti-virus mechanism 6 can apply the techniques described hereinafter to resist mass mailing malware," and also notes that page 9, lines 21-22 of the specification states that "the general purpose computer 200 operating under control of a suitable computer program may perform the above described techniques" (emphasis added). For these and other reasons, support for the combination of (i), (ii), and (iii) claimed in each of the independent claims is present. Of course, such citations are set forth by way of example only and should not be construed limiting to the claims in any manner.

In the Examiner's Answer mailed 10/05/2007, the Examiner has argued that "appellants have only pointed at the general statements in the specification," and that "[n]either of these statements explicitly or implicitly provides support for identifying all of (i), (ii), and (iii) **together**." The Examiner has further argued that "the section of the specification which supports (i), (ii), and (iii), located at Page 7 Line 30 - Page 8 Line 15, only supports identification of these conditions in the alternative."

Appellant respectfully disagrees. As shown in item 14 of Figure 3 of appellant's specification, it is determined whether a "percentage of the total address book addresses who are being addressed by the new e-mail message" exceeds a threshold (see also page 6, line 27 - page 7, line 1 of the specification - emphasis added). As further shown, item 28 of Figure 3 discloses that "the email message is added to a quarantine queue" (see also page 7, lines 23-25 of the specification).

Moreover, with respect to the description of Figure 4 of appellant's specification, page 7, lines 31-34 teach that "[a]t step 30 the system waits to receive an e-mail message issued from step 28 of Figure 3," and that "[w]hen an e-mail message is received, step 32 serves to compare the received e-mail message with any existing messages currently held within the quarantine queue"

(emphasis added). Page 8, lines 1-3 of the specification specifically states that such comparison may "identif[y] as the same any messages sharing above a predetermined threshold level of content" (emphasis added).

Thus, for at least the reasons noted above, appellant's specification, as originally filed, clearly supports the combination of (i), (ii), and (iii) claimed in each of the independent claims. Again, it should be noted that such citations are set forth by way of example only and should not be construed limiting to the claims in any manner.

Issue # 2:

The Examiner has rejected Claims 1-4, 6-12, 14-20, and 22-28 under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement.

Group #1: Claims 1-4, 6-12, 14-20, and 22-28

The Examiner has argued that "there is support for each of (i), (ii) and (iii) in the alternative, as shown in page 7 line 30 – page 8 line 15 of the present specification, but never as a combination." Appellant respectfully disagrees and points out that page 6, lines 12-13 of the specification states that "the anti-virus mechanism 6 can apply the techniques described hereinafter to resist mass mailing malware," and also notes that page 9, lines 21-22 of the specification states that "the general purpose computer 200 operating under control of a suitable computer program may perform the above described techniques" (emphasis added). Thus, support for the combination of (i), (ii), and (iii) claimed in each of the independent claims is present. Of course, such citations are set forth by way of example only and should not be construed limiting to the claims in any manner.

In the Examiner's Answer mailed 10/05/2007, the Examiner has argued that "appellants have only pointed at the general statements in the specification," and that "[n]either of these statements explicitly or implicitly provides support for identifying all of (i), (ii), and (iii) **together**." The Examiner has further argued that "the section of the specification which supports

(i), (ii), and (iii), located at Page 7 Line 30 - Page 8 Line 15, only supports identification of these conditions in the alternative."

Appellant respectfully disagrees. As shown in item 14 of Figure 3 of appellant's specification, it is determined whether a "percentage of the total address book addresses who are being addressed by the new e-mail message" exceeds a threshold (see also page 6, line 27 - page 7, line 1 of the specification - emphasis added). As further shown, item 28 of Figure 3 discloses that "the email message is added to a quarantine queue" (see also page 7, lines 23-25 of the specification).

Moreover, with respect to the description of Figure 4 of appellant's specification, page 7, lines 31-34 teach that "[a]t step 30 the system waits to receive an e-mail message issued from step 28 of Figure 3," and that "[w]hen an e-mail message is received, step 32 serves to compare the received e-mail message with any existing messages currently held within the quarantine queue" (emphasis added). Page 8, lines 1-3 of the specification specifically states that such comparison may "identif[y] as the same any messages sharing above a predetermined threshold level of content" (emphasis added).

Thus, for at least the reasons noted above, appellant's specification, as originally filed, clearly supports the combination of (i), (ii), and (iii) claimed in each of the independent claims. Again, it should be noted that such citations are set forth by way of example only and should not be construed limiting to the claims in any manner.

Issue # 3:

The Examiner has rejected Claims 1-3, 7, 9-11, 15, 17-19, 23, and 26 under 35 U.S.C. 103(a) as being unpatentable over Bates et al. (U.S. Patent No. 6,779,021), in view of Marsh (U.S. Patent No. 6,763,462).

Group #1: Claims 1-3, 7, 9-11, 15, 17-19, and 23

In order to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the

knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*,947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

With respect to the third element of the *prima facie* case of obviousness, and particularly with respect to the independent claims, the Examiner has relied on Col. 9, lines 3-19 from the Bates reference to make a prior art showing of appellant's claimed "comparison logic operable to compare said e-mail message with at least one of an address book of a sender of said e-mail message and one or more previously generated e-mail messages from said client computer" (see this or similar, but not necessarily identical language in the independent claims).

> 'Block 94 illustrates comparing the new e-mail source address with the source addresses of e-mail received during a designated "B" time period. In particular, a rule designating the "B" time period is preferably included in spam filtering rules for the filter and may be adjusted by the prediction application executing on the server or by an alternate source. Next, block 98 depicts a determination as to whether or not the number of users receiving e-mail from the same source address during the "B" time period is greater than a designated "C" number of recipients. If the number of users receiving e-mail from the same source address during the "B" time period is greater than a designated "C" number of recipients, then the process passes to block 120. If the number of users receiving e-mail from the same source address during the "B" time period is not greater than a designated "C" number of recipients, then the process passes to block 100.' (Col. 9, lines 3-19)

Appellant respectfully notes that the excerpt from Bates relied on by the Examiner simply teaches 'comparing the new e-mail source address with the source addresses of e-mail received during a designated "B" time period' (emphasis added). Clearly, in Bates, a new e-mail source address is only compared with e-mail received, which does not meet "compar[ing] said e-mail message with at least one of an address book of a sender of said e-mail message and one or more previously generated e-mail messages from said client computer" where "said previously generated e-mail messages [are held] in a quarantine queue for at least a predetermined quarantine period prior to being sent from said client computer," in the context specifically claimed by appellant (emphasis added).

In the Examiner's Answer mailed 10/05/2007, the Examiner has argued that "Bates disclosed in Col. 6, Lines 64-67 that as *'an additional feature, prediction application 42 may also* ***analyze out-going e-mail in the same manner as in-coming e-mail*** *to predict the likelihood of each outgoing e-mail as spam.'"* Specifically, the Examiner has argued that "in Bates, when analyzing an e-mail which is **out-going**, it is clear that the e-mail 'received' by the prediction application 42 would have been generated in the client, and therefore the new email 'source address', which is part of the new e-mail, is compared with the 'received' out-going mail." Also in the Examiner's Answer mailed 10/05/2007, the Examiner has argued that "Marsh clearly teaches comparing an e-mail message with an address book of a sender of said e-mail message, as seen in the Background of Marsh and Col. 2, Line 34 - Col. 3 Line 65." Further, the Examiner has argued that "Bates, in Col. 9 Lines 3-5, disclosed comparing new e-mail with the source addresses of e-mail received during a designated 'B' time period," and that such "'list' of source addresses falls within the scope of an address book." Appellant respectfully disagrees.

Additionally, with respect to the independent claims, the Examiner has relied on Col. 9, line 64 – Col. 10, line 10 from the Bates reference to make a prior art showing of appellant's claimed "identifying logic operable to identify whether…said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of said previously generated e-mail messages being sent to more than a threshold number of addressees specified within said address book" (see this or similar, but not necessarily identical language in the independent claims).

> "Block 112 illustrates comparing the content of e-mails that are the same size as the new e-mail with the content of the new e-mail. Spam filtering rules designated at the server preferably designate grouping of previously received e-mails that may be utilized for size comparison. Thereafter, block 114 depicts a determination as to whether or not substantial similarities in content are found between the new e-mail and a particular amount of same sized e-mail. If there are substantial similarities in content between the new e-mail and a particular amount of same sized e-mail, then the process passes to block 120. If there are not substantial similarities in content between the new e-mail and a particular amount of same sized e-mail, then the process passes to block 116." (Col. 9, line 64 - Col. 10, line 10)

Appellant respectfully asserts the excerpt from Bates relied on by the Examiner merely discloses "comparing the content of e-mails that are the same size as the new e-mail with the content of the

new e-mail" (emphasis added). However, appellant claims a technique where "said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of said previously generated e-mail messages being sent to more than a threshold number of addressees specified within said address book," in the context claimed (emphasis added). Appellant notes that simply nowhere in Bates is there any disclosure of "e-mail messages being sent to more than a threshold number of addressees specified within said address book," in the context claimed by appellant (emphasis added).

Additionally, appellant respectfully points out block 98 in Fig. 4A of the Bates reference, which 'depicts a determination as to whether or not the number of users receiving e-mail from the same source address during the "B" time period is greater than a designated "C" number of recipients' (Col. 9, lines 9-12). In Fig. 4A, if the determination in block 98 results in an affirmative, or "YES," result, the process **skips block 114**, which "depicts a determination as to whether or not substantial similarities in content are found between the new e-mail and a particular amount of same sized e-mail" (Col. 10, lines 1-4), and instead proceeds directly to block 120, which "illustrates marking the new e-mail as predicted spam" (Col. 10, lines 17-18). Clearly, this fails to meet, and even *teaches away* from appellant's claimed "identifying logic operable to identify whether...said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of said previously generated e-mail messages being sent to more than a threshold number of addressees specified within said address book," as claimed (emphasis added).

In the Examiner's Answer mailed 10/05/2007, the Examiner has argued that "Bates discloses determining whether or not the number of users receiving e-mail from the same source address during a time period is greater than a designated number of recipients, as is seen in Col. 9 Lines 3-19." The Examiner has also argued that "[b]ecause the 'source address' is a portion of an e-mail message, as is the recipient address, and because the messages being 'tallied' all have the same source address, then these tallied messages have at least that level of similarity with one another, without being identical." Still yet, the Examiner has argued that "because the list of users who have received e-mail from the same source address during the 'B' time period constitutes an address book, Bates has disclosed this particular limitation."

Appellant respectfully disagrees. An address book, which includes a list of users who have received e-mail from the same source address, as noted by the Examiner, fails to meet appellant's claimed "previously generated e-mail messages being sent to more than a threshold number of addressees specified within said address book," as claimed (emphasis added). In addition, Bates only discloses "sources addresses of e-mail received during a designated 'B' time period" (Col. 9, lines 4-5), which clearly does not even suggest any sort of threshold, let alone specifically meet appellant's claimed "previously generated e-mail messages being sent to more than **a threshold number** of addressees specified within said address book," as claimed (emphasis added).

Also in the Examiner's Answer mailed 10/05/2007, the Examiner has argued that "Marsh teaches, in Col. 1 Lines 35-53 and Col. 2 Line 34 - Col. 3 Line 34, a method for identifying viral spam which involves determining whether a message is addressed to more than [a] certain number of addresses from the senders address book, which is indicative of a virus attempting to replicate itself through e-mail propagation," and that "[o]ne of ordinary skill in the art...would recognize that by utilizing the teachings of Marsh in the spam detection system of Bates, by determining whether a threshold number of addresses from the senders address book are included as recipients of an e-mail message, that the message can be predicted as viral spam."

Appellant respectfully disagrees and asserts that the excerpts from Marsh relied on by the Examiner merely disclose viruses that spread by sending electronic mail" (Col. 1, line 51), that "potential virus activity may be detected by finding a specified number of the e-mail addresses corresponding to the generated random numbers in the recipients list of an outgoing message," and only that a "user may be notified of possible virus activity" (Col. 3, lines 24-35 – emphasis added). Simply nowhere in the excerpts from Marsh relied on by the Examiner is there any disclosure of "previously generated e-mail messages being sent to more than a threshold number of addressees specified within said address book" which are utilized in order to "identify whether...said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of said previously generated e-mail messages," as claimed (emphasis added). Clearly, finding a specified number of e-mail addresses corresponding to generated random number in the recipients list of an outgoing message, as in Marsh, simply fails to suggest "previously generated e-mail messages being sent to more than a

threshold number of addressees specified within said address book," as claimed (emphasis added).

Further, appellant respectfully points out that Bates only discloses that "multiple e-mails are received at a network server," and that the "e-mails are analyzed to determine patterns of similarity" (Col. 3, lines 55-57). Clearly, only determining whether any received e-mails are similar, as in Bates, fails to specifically teach "previously generated e-mail messages being sent to more than a threshold number of addressees specified within said address book" that are utilized to "identify whether...said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of said previously generated e-mail messages," as claimed (emphasis added).

Still yet, in the Examiner's Answer mailed 10/05/2007, the Examiner has argued that "[r]egarding appellant's [above] argument that in the system of Bates, when step 94 of Fig. 4A results in a 'YES' for step 98, that step 114 of Bates, which compares for substantial similarities between e-mails, is not executed, and therefore Bates does not teach, but rather teaches away from, performing both step 98 and 114, the [E]xaminer disagrees." Specifically, the Examiner has argued that "as shown in Fig. 4A, as long as the determinations from step 98 - step 110 continue to result in 'NO', the determinations are made," and that appellant's "example when step 98 results in 'YES' is merely one [of] the 'scenarios' disclosed by Bates, and not the scenario being relied upon in rejecting the claims." The Examiner has further argued that "in no way does this one scenario teach away from the scenario when both step 98 and step 114 are performed," and that "for any message which...does not have recipients on the inclusion list, but is determined to be normal e-mail, and not spam, steps 98 and 114 are performed."

Appellant respectfully disagrees. Figure 4A in Bates shows, in block 114, determining whether or not substantial similarities in content are found between the new e-mail and a particular amount of same sized e-mail (Col. 10, lines 1-4) only if it is determined in block 98 that the number of users receiving e-mail from the same source address during the "B" time period is NOT greater than a designated "C" number of recipients (Col. 9, lines 9-12). Appellant respectfully asserts that Bates simply does not disclose any scenario other than determining whether substantial similarities are found between a new e-mail and a particular amount of same

sized e-mail (block 114) if it is determined that the number of users receiving e-mail from the same source address during the "B" time period is not greater than a designated "C" number of recipients. Thus, Bates clearly does not meet, and actually *teaches away* from, appellant's claimed "identifying logic operable to identify whether...said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of said previously generated e-mail messages being sent to more than a threshold number of addressees specified within said address book," as claimed (emphasis added).

To this end, appellant respectfully asserts that the Marsh and Bates references, as relied on by the Examiner, do not teach or suggest alone or in combination appellant's specific claim language. Thus, the third element of the *prima facie* case of obviousness has not been met, for at least the reasons noted above.

With respect to the first element of the *prima facie* case of obviousness and, in particular, the obviousness of combining the aforementioned references, the Examiner has argued that it would have been obvious to combine Bates with Marsh because 'the ordinary person skilled in the art would have been motivated to provide means of detecting viral spam as suggested by Marsh, as well as giving the user the final say in what is to be done with detected viral spam...[and that] in this combination it would be obvious that the messages would be held in a "quarantine" for a predetermined amount of time prior to sending in order for the user to have the option of deleting the messages detected as being viral spam without sending the messages.' To the contrary, appellant respectfully asserts that it would not have been obvious to combine the teachings of the Bates and Marsh references, especially in view of the vast evidence to the contrary.

For example, the Bates reference teaches that "[i]n accordance with the present invention, multiple e-mails are received at a network server intended for multiple clients served by the network server" (see Abstract) and that '[b]lock 92 depicts a determination as to whether or 1C not the number of recipients of the new e-mail is greater that a designated "A" number of recipients...[where] a rule designating the "A" number of recipients is preferably included in spam filtering rules for the server' (see Bates Col. 8, lines 56-60). On the other hand, the Marsh reference teaches that "the virus detection utility 104 may be an add in program organized into a conventional format such as a plug-in for the e-mail application 102" where "[f]or example, the

virus detection utility 104 [is] stored as a dynamic link library (DLL) file and...include[s] routines to execute in conjunction with the e-mail application 102 to perform specific operations" (see Marsh Col. 2, lines 26-33).

Clearly, in Marsh, the virus detection utility runs on clients in conjunction with e-mail applications located on such clients, and utilizes client-based information (e.g. address books), whereas, in Bates, a server is used to receive e-mails sent to clients and to predict undesirable e-mails utilizing rules stored on the server. Thus, Marsh clearly *teaches away* from Bates. Appellant respectfully points out that it is improper to combine references where the references *teach away* from their combination. *In re Grasselli*, 713 F.2d 732, 743, 218 USPQ 769, 779 (Fed. Circ. 1983).

In the Examiner's Answer mailed 10/05/2007, the Examiner has argued that "simply because Marsh disclosed a preferred embodiment on a client, while Bates disclosed a preferred embodiment on a server, does not teach away from [the] suggested combination."

Appellant respectfully disagrees and again emphasizes that in Marsh, the virus detection utility runs on clients in conjunction with e-mail applications located on such clients, and utilizes client-based information (e.g. address books), whereas, in Bates, a server is used to receive e-mails sent to clients and to predict undesirable e-mails utilizing rules stored on the server. Thus, Marsh does in fact *teach away* from Bates.

Also in the Examiner's Answer mailed 10/05/2007, the Examiner has argued that "Bates clearly teaches that a pc can be both a client and a server (See Bates Col. 1 Lines 21-26), that it is known for e-mail software applications on the client to perform the filtering of unsolicited e-mail (See Bates Col. 2 Lines 8-11), that the teachings of Bates can be applied to out-going email...such as those that automatically transmit themselves utilizing client e-mail address books (see Bates Col. 6 Line 64 [to] Col. 7 Line 6), and that unsolicited sending of e-mail can unnecessarily utilize data storage space on servers (See Bates Col. 2 Lines 1-2)." The Examiner has concluded that "[b]ased on these teachings alone, it is clear that Bates does not teach away from filtering e-mail at the client."

Appellant respectfully disagrees. Bates discloses that "[i]n many networks, a primary function of a server is receiving e-mail addressed to clients and transmitting e-mail composed received from clients" (Col. 1, lines 49-51). Thus, Bates clearly relates to a server on a network which transmits e-mail addressed to clients that has been received from clients. In fact, appellant respectfully points out Figure 2 of Bates illustrating "a network system in accordance with the method, system and program of the present invention" (Col. 4, lines 21-23 - emphasis added), which clearly shows the network server 40 separate from the client systems 60a-n. Thus, Bates only discloses a server that receives e-mail from clients which is addressed to other clients and that the server transmits the received e-mail to such addressee clients, which does *teach away* from Marsh's system in which the virus detection utility runs on clients in conjunction with e-mail applications located on such clients.

Moreover, in the Examiner's Answer mailed 10/05/2007, the Examiner has argued that "one of ordinary skill in the art would have recognized, based upon these teachings of Bates, that in order to unnecessarily utilize data storage space on servers, that the filtering of out-going e-mail should be performed at the client utilizing the clients e-mail software packages."

Appellant respectfully disagrees. For example, appellant notes that Bates does disclose that the "unsolicited sending a receiving of e-mail can unnecessarily utilize data storage space on servers" (Col. 2, lines 1-2). However, in response to such problem, Bates does not suggest that "in order to unnecessarily utilize data storage space on servers,...the filtering of out-going e-mail should be performed at the client utilizing the clients e-mail software packages," as alleged by the Examiner. Appellant respectfully asserts that Bates only teaches that "[i]n view of the foregoing [including the unnecessary usage of data storage space on server by unsolicited e-mails], it would be advantageous to provide a method for automatically analyzing electronic mail as it arrives at a network server" (Col. 3, lines 34-36 - emphasis added). Thus, it would not have been obvious to perform the "filtering of out-going e-mail...at the client utilizing the clients e-mail software packages," as argued by the Examiner.

To this end, appellant respectfully asserts that the first element of the *prima facie* case of obviousness has also not been met, for at least the reasons noted above.

Thus, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since it would be *unobvious* to combine the references, as noted above, and the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Group #2: Claim 26

With respect to dependent Claim 26, the Examiner has relied on Col. 1, line 66 – Col. 2, line 7 in Bates to make a prior art showing of appellant's claimed technique "wherein said e-mail message is identified as potentially containing malware when said e-mail message and said previously generated e-mail messages share a common attachment."

> "The sending and receiving of unsolicited e-mail messages are increasing problems for both ISPs and corporations. In particular, unsolicited sending and receiving of e-mail can unnecessarily utilize data storage space on servers and for ISPs unsolicited mail reduces customer satisfaction. In addition, unsolicited mail may includes viruses, worms, or other destructive attachments that can easily be transmitted within a server upon activation at a single client within a network." (Col. 1, line 66 - Col. 2, line 7)

Appellant respectfully asserts that such excerpt from Bates only discloses that "other destructive attachments…can easily be transmitted within a server upon activation of a single client within a network." Clearly, only mentioning an attachment, as in Bates, does not even suggest appellant's specific claim language, namely that "said e-mail message is identified as potentially containing malware **when** said e-mail message and said previously generated e-mail messages share a common attachment," as claimed (emphasis added).

In the Examiner's Answer mailed 10/05/2007, the Examiner has argued that "Bates teaches determining whether a certain number of users receive 'the same email'…and if so predicting it as spam (See Bates Col. 7 Lines 23-29)." The Examiner has further argued that "Bates, in Col. 2 Lines 3-7, disclosed that 'unsolicited mail may includes…destructive attachments," such that "by determining whether a certain number of users receives 'the same email'…Bates also determines whether any attachments in the e-mails are the same."

Appellant respectfully disagrees. In Col. 7, lines 22-36 of Bates, Bates discloses that "during the first filtering process, prediction application 42 looks for an unusually large number of users receiving the same e-mail from a particular user address in a given time period," and that "[i]n particular, prediction application 42 not only checks the "TO" list to see how many users an e-mail is sent to, but checks to see if a single user address (or domain) is sending many tailored spam notes to individuals serviced by network server 40" (emphasis added). Such excerpt from Bates also discloses that "[t]herefore, in a second filtering process if a large number of tailored e-mails are received from a single user address or domain, prediction application 42 preferably compares the messages to determine similarities in content" such that "[i]f there is a large percentage of similarity in content, then prediction application 42 preferably marks these e-mails as predicted spam" (emphasis added). Thus, Bates only discloses determining e-mails to be spam if such e-mails have a large percentage of similarity in content, which clearly does not specifically disclose that "said e-mail message is identified as potentially containing malware when said e-mail message and said previously generated e-mail messages share a common attachment," as claimed (emphasis added).

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since it would be *unobvious* to combine the references, as noted above, and the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Issue # 4:

The Examiner has rejected Claims 4, 6, 12, 14, 20, 22, and 27-28 under 35 U.S.C. 103(a) as being unpatentable over Bates et al. (U.S. Patent No. 6,779,021), in view of Marsh (U.S. Patent No. 6,763,462), and further in view of Bates et al. (U.S. Patent No. 6,785,732) (Bates2).

Group #1: Claims 4, 6, 12, 14, 20, and 22

Appellant respectfully asserts that such claims are not met by the prior art for the reasons argued with respect to Issue #3, Group #1.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since it would be *unobvious* to combine the references, as noted above, and the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Group #2: Claim 27

With respect to dependent Claim 27, the Examiner has relied on Col. 8, paragraph 1 in Bates2 to make a prior art showing of appellant's claimed technique "wherein a message is sent to a malware computer program provider to provide a warning of new malware outbreaks when said e-mail message is identified as potentially containing malware."

> "...Method 400 begins when a web client requests information that normally would flow through the web server to the web client (step 410). If the request does not require virus checking (step 420=NO), the requested information is sent to the web client (step 480). If the request requires virus checking (step 420=YES), a virus check is performed on the requested information (step 430). If no virus is found (step 440=NO), the requested information is sent to the web client (step 480). If a virus is found (step 440=YES), the web client is notified of the virus (step 450), and an entry is made in the virus information database (step 460) regarding the name of the virus, type, when detected, etc. Finally, the appropriate authorities may be notified of the virus (step 470). The term "appropriate authorities" is a broad term that encompasses anyone who may need to know about the occurrence of a virus, including a network administrator of a local area network, a web site administrator, a contact person in a virus detection company, and appropriate law enforcement officials, such as local, state, federal, and international law enforcement agencies." (Col. 8, paragraph 1 – emphasis added)

Appellant respectfully asserts that the excerpt from Bates2 relied upon by the Examiner merely discloses that "[i]f a virus is found... the web client is notified of the virus (step 450)" and that "the appropriate authorities may be notified of the virus" (emphasis added). However, the mere disclosure that if a virus is found, the appropriate authorities may be notified of the virus, as in Bates2, simply fails to even suggest a technique "wherein a message is sent to a malware computer program provider to provide a warning of new malware outbreaks when said e-mail message is identified as potentially containing malware," as claimed by appellant (emphasis added). Clearly, the mere disclosure of notifying the appropriate authorities of the found virus,

as in Bates2, simply fails to suggest "provid[ing] a warning of new malware outbreaks," in the manner as claimed by appellant (emphasis added).

In the Examiner's Answer mailed 10/05/2007, the Examiner has argued that "[w]hen malware is detected in a new e-mail, as taught by Bates and Marsh, because the e-mail is a new e-mail, the malware in the e-mail is a new instance of the malware, and therefore is a new malware outbreak." Appellant respectfully disagrees.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since it would be *unobvious* to combine the references, as noted above, and the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Group #3: Claim 28

With respect to dependent Claim 28, the Examiner has relied on Col. 8, paragraph 1 in Bates2 (reproduced above) to make a prior art showing of appellant's claimed technique "wherein said message to said malware computer program provider includes a copy of said e-mail message."

Appellant respectfully asserts that the excerpt from Bates2 relied upon by the Examiner merely discloses that "[i]f a virus is found... the web client is notified of the virus (step 450)" and that "the appropriate authorities may be notified of the virus" (emphasis added). However, the general disclosure that if a virus is found, the appropriate authorities may be notified of the virus, as in Bates2, simply fails to even suggest a specific technique "wherein said message to said malware computer program provider includes a copy of said e-mail message," as claimed by appellant (emphasis added). Clearly, the mere disclosure of notifying the appropriate authorities of the found virus, as in Bates2, simply fails to suggest that the "message to said malware computer program provider includes a copy of said e-mail message," in the manner as claimed by appellant (emphasis added).

In the Examiner's Answer mailed 10/05/2007, the Examiner has argued that "the [E]xaminer has relied upon what would have been common sense to the ordinary person skilled in the art of

malware detection, in that upon sending a message notifying a virus detection company of detection of an e-mail infected by malware, it would have been common sense to include the infected email in the message in order to allow the virus detection company to analyze the virus for future detection."

Appellant respectfully disagrees. Bates2 only generally discloses that "[i]f a virus is found...the appropriate authorities may be notified of the virus" (Col. 8, lines 11-16 - emphasis added). In fact, appellant notes that Bates actually discloses that "[i]f a virus is found...the e-mail message is deleted...and a separate e-mail is sent to the intended recipient of the e-mail informing the recipient that the deleted e-mail message contained a virus and was automatically deleted" (Col. 9, lines 31-38). Thus, Bates only generally teaches notifying appropriate authorities of a virus, and that an e-mail message is deleted when a virus is found in such e-mail message. Simply nowhere does Bates2 even suggest that the "message to said malware computer program provider includes a copy of said e-mail message," in the manner as claimed by appellant (emphasis added).

In response to the Examiner's apparent reliance on Official Notice in rejecting appellant's specific claim language, appellant again points out the remarks above that clearly show the manner in which some of such claims further distinguish the prior art relied on by the Examiner. Appellant thus formally requests a specific showing of the subject matter in ALL of the claims in any future action. Note excerpt from MPEP below.

"If the [appellant] traverses such an [Official Notice] assertion the examiner should cite a reference in support of his or her position." See MPEP 2144.03.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since it would be *unobvious* to combine the references, as noted above, and the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Issue # 5:

The Examiner has rejected Claims 8, 16, and 24 under 35 U.S.C. 103(a) as being unpatentable over Bates et al. (U.S. Patent No. 6,779,021), in view of Marsh (U.S. Patent No. 6,763,462), and further in view of Kouznetsov (U.S. Patent No. 6,725,377).

Group #1: Claims 8, 16, and 24

Appellant respectfully asserts that such claims are not met by the prior art for the reasons argued with respect to Issue #3, Group #1.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since it would be *unobvious* to combine the references, as noted above, and the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Issue # 6:

The Examiner has rejected Claim 25 under 35 U.S.C. 103(a) as being unpatentable over Bates et al. (U.S. Patent No. 6,779,021), in view of Marsh (U.S. Patent No. 6,763,462), and further in view of Radatti (U.S. Patent No. 6,763,467).

Group #1: Claim 25

With respect to dependent Claim 25, the Examiner has relied on Col. 1, lines 36-48 of the Radatti reference to make a prior art showing of appellant's claimed technique "wherein said e-mail message is identified as potentially containing malware only if said e-mail message includes an executable element, to speed processing."

> "Virus, worms, and trojan horses can infect an internal network or single computer system when the internal network or computer system executes a program from the external network that contains the hostile algorithm. All binary executables, unreviewed shell scripts, and source code accessed from an external network may contain worms, viruses, or trojan horses. In addition, outside binary executables, shell scripts, and scanned source code may enter an internal network or single computer system through an E-mail attachment. Also, executables can be directly accessed from an external network through the IFTP program, a

> world-wide web browser, or an outside contractor whose network already has been compromised." (Col. 1, lines 36-48)

Specifically, appellant notes that the Examiner has argued that "Radatti teaches that only executable code may contain malware." Appellant respectfully disagrees and points out that the excerpt from Radatti merely discloses that "[a]ll binary executables, unreviewed shell scripts, and source code accessed from an external network may contain worms, viruses, or trojan horses" and that "outside binary executables, shell scripts, and scanned source code may enter an internal network or single computer system through an E-mail attachment" (emphasis added). Clearly, disclosing that binary executables may contain worm, viruses, or Trojan horses, as in Radatti, does not suggest that "only executable code may contain malware," as noted by the Examiner (emphasis added). Furthermore, simply disclosing that executables may contain worms, viruses, or Trojan horses, as in Radatti, does not specifically teach any sort of e-mail, let alone meet appellant's specifically claimed technique "wherein said e-mail message is identified as potentially containing malware only if said e-mail message includes an executable element, **to speed processing**," as claimed by appellant (emphasis added).

In the Examiner's Answer mailed 10/05/2007, the Examiner has argued that "[b]ecause it was well known that malware requires an executable element, and more specifically that e-mail propagated viruses, as are being detected in the combination of Bates and Marsh, require an executable payload, it would have been obvious to the ordinary person skilled in the art at the time of invention to have only identified an e-mail as potentially containing malware if it contained an executable payload" in order to prevent "creat[ion] [of] unnecessary false positives." The Examiner has also argued that "because all malware must have an executable element, it would have been obvious to one of ordinary skill in the art to not identify an e-mail as potentially containing malware if it did not have an executable element."

First, appellant respectfully asserts that simply alleging that malware requires an executable element, as noted by the Examiner, does not support the Examiner's obviousness argument with respect to appellant's claimed technique "wherein said e-mail message is identified as potentially containing malware only if said e-mail message includes an executable element, to speed processing," as claimed (emphasis added). Appellant respectfully asserts that simply because some executable elements may include malware, does not make it obvious to identify an "e-mail

message...as potentially containing malware **only if** said e-mail message includes an executable element," as claimed (emphasis added). In fact, appellant respectfully points out that none of the prior art references, as relied on by the Examiner, disclose that an "e-mail message is identified as potentially containing malware **only if** said e-mail message includes an executable element, to speed processing," as appellant claims (emphasis added).

Second, appellant respectfully asserts that simply alleging that "because all malware must have an executable element, it would have been obvious to one of ordinary skill in the art to not identify an e-mail as potentially containing malware if it did not have an executable element," as noted by the Examiner, does not imply the converse. For example, not identifying an e-mail as potentially containing malware if it did not have an executable element, as noted by the Examiner, does not imply that an "e-mail message is identified as potentially containing malware **only if** said e-mail message includes an executable element, to speed processing," as appellant claims (emphasis added).

Thus, in response to the Examiner's apparent reliance on Official Notice in rejecting appellant's specific claim language, appellant again points out the remarks above that clearly show the manner in which some of such claims further distinguish the prior art relied on by the Examiner. Appellant thus formally requests a specific showing of the subject matter in ALL of the claims in any future action. Note excerpt from MPEP 2144.03, cited above.

Again, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since it would be *unobvious* to combine the references, as noted above, and the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P462).

Respectfully submitted,

By: /KEVINZILKA/ Date: December 5, 2007
Kevin J. Zilka
Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660